資安監控有效性驗證

行政院國家資通安全會報技術服務中心

110年

【普通】

大綱

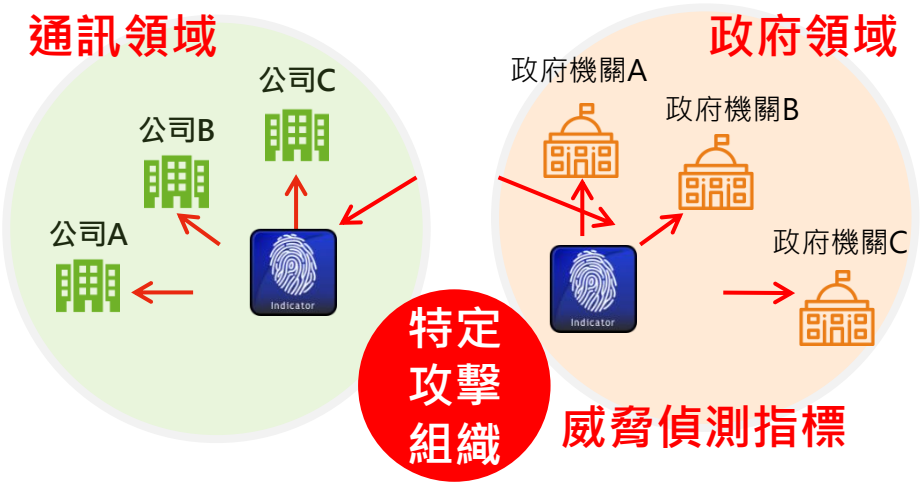
- 前言
- 政府領域聯防監控情資收容與分析
- SOC監控有效性驗證
- SOC監控有效性現況
- SOC監控防護建議
- 機關配合事項

政府機關資安防護現況

- 在資安防護策略上，若僅參採國外威脅情資，常因駭客組織具地域性，許多情資部署後成效並不顯著
- 針對攻擊我國之駭客組織威脅情資，雖已於相關單位間進行分享，惟仍未能發揮資安聯防之綜效

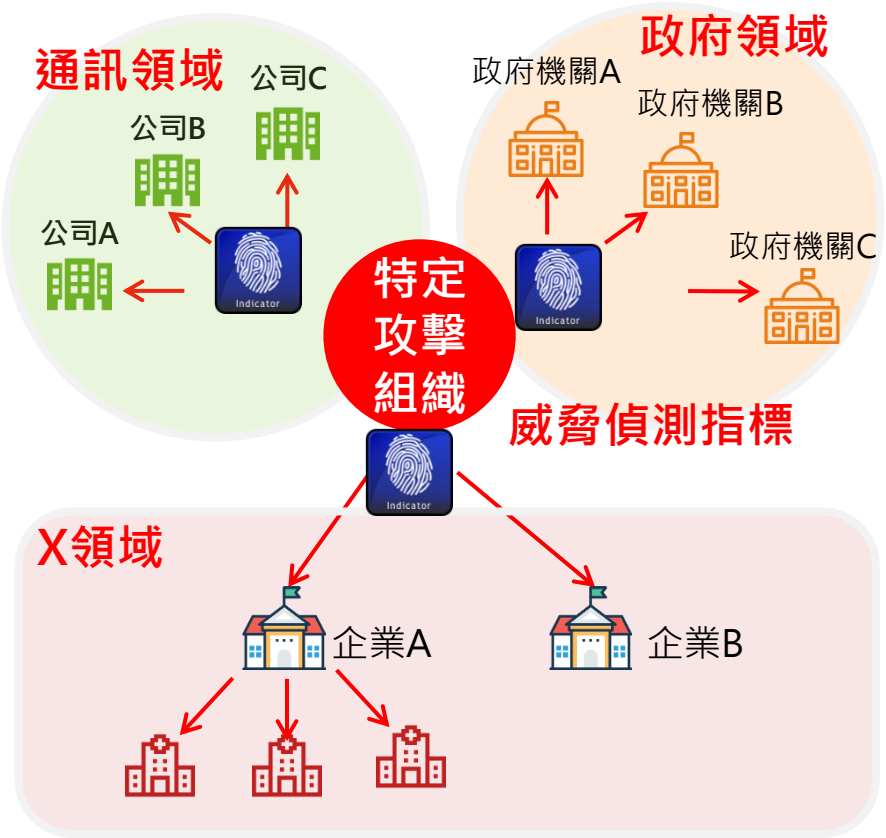
近期駭客攻擊案例

- **政府領域於5月偵測到經濟能源類機關遭使用Cobalt Strike工具，透過DNS Tunnel手法進行資料竊取與命令控制**
- **經事後蒐集相關案例進行分析，發現OO電商受駭偵測指標資訊wystedba.top與該事件相關**



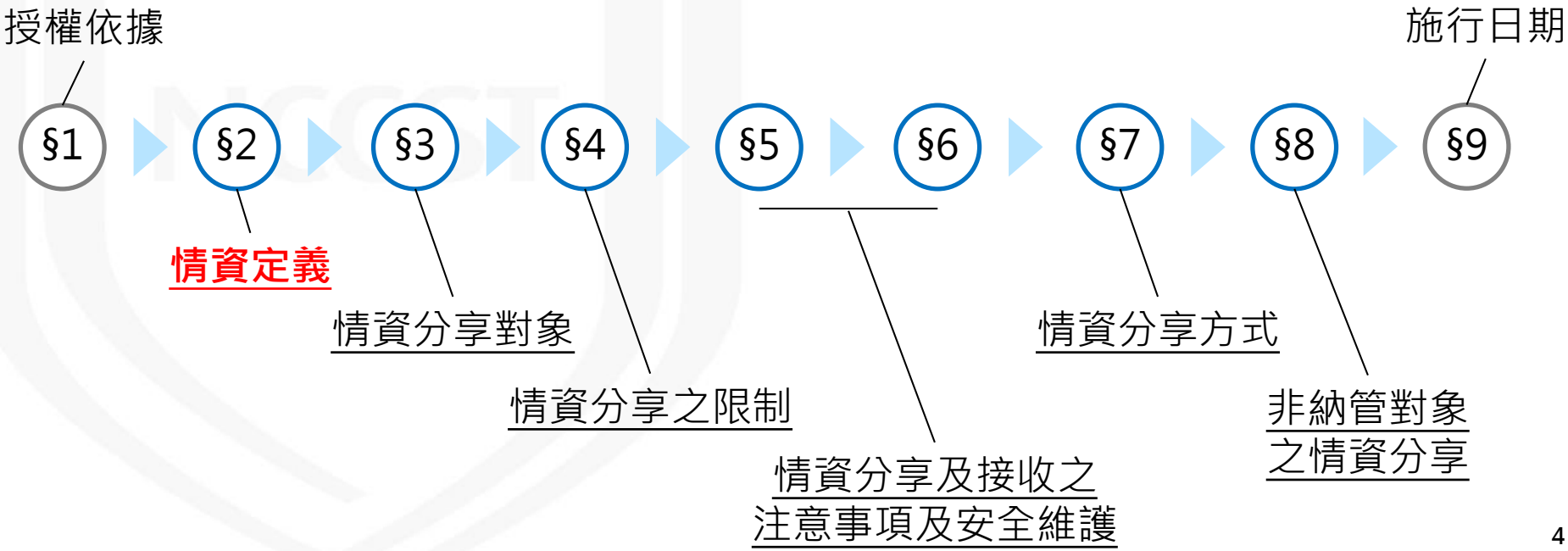
強化政府機關資安聯防能量

- 政府機關已具備第一線資安監控防護能量，現需擴大推動資安聯防機制
  - 蒐集公務機關第一線威脅情資，進行**即時分析**，萃取威脅指標與手法，產製與共享**自主聯防情資**
  - 提供政府領域及早進行部署偵測
  - 協助彙整跨領域情資，掌握跨域資安威脅現況



資通安全管理法相關規定

- 資通安全管理法(第8條)
  - 主管機關應建立資通安全情資分享機制
  - 前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之
- 資通安全情資分享辦法



資安情資定義內容

§1 ▶ §2 ▶ §3 ▶ §4 ▶ §5 ▶ §6 ▶ §7 ▶ §8 ▶ §9

一、	惡意偵察/情蒐活動	惡意活動偵測紀錄、資安監控單、情資分析單、疑似攻擊探測紀錄、關聯分析結果
二、	系統安全漏洞	漏洞資訊
三、	使安控失效或利用漏洞方法	攻擊手法
四、	惡意程式相關資訊	惡意程式、中繼站資訊、受駭者資訊、惡意IP/DN、惡意郵件來源
五、	資安事件之損害或影響	中繼站黑名單阻擋統計
六、	偵測、預防或降低損害措施	惡意程式分析報告、惡意活動趨勢分析、攻擊應變措施
七、	其他技術性資訊	資安趨勢報告、領域監控分析報告

資通安全責任等級分級辦法

- 於修正草案中，監控範圍應包括「端點偵測及回應機制」與「資通安全防護」之辦理項目、目錄服務系統及機關核心資通系統等之資訊設備紀錄與服務/應用程式紀錄

辦理項目	辦理內容	資安責任等級				
		A	B	C	D	E
資通安全威脅偵測管理機制	**完成威脅偵測機制建置，並持續維運**	★	★			
	公務機關依主管機關指定之方式提交監控管理資料	★	★			
資通安全防護 (啟用，並持續使用及適時進行軟、硬體之必要更新或升級)	• 防毒軟體 • 網路防火牆 • 電子郵件過濾機制(具有郵件伺服器者)	★	★	★	★	
	• 入侵偵測及防禦機制(IDS/IPS) • 應用程式防火牆(具有對外服務之核心資通系統者)	★	★			
	• APT攻擊防禦機制	★				

「★」表示：機關初次受核定或等級變更後一年內需完成項目

資安情資來源類型

- 資通安全威脅偵測管理機制
  - 應包含資通安全防護項目
    - 現有資安防護設施與對外服務核心資通系統之資安防護機制

項次	法定資通安全防護項目
1	防毒軟體
2	網路防火牆
3	應用程式防火牆
4	入侵偵測及防禦機制
5	進階持續性威脅攻擊防禦措施
6	電子郵件過濾機制

- 惡意偵察或情蒐活動相關情資
  - 如DNS警示紀錄、EDR端點防護、MDR防護紀錄、DDoS防護機制及HoneyPot機制等

項次	額外資安偵蒐機制
1	DNS警示紀錄
2	EDR端點防護*
3	MDR防護紀錄
4	DDoS防護機制
5	HoneyPot機制

***EDR端點防護**已納入資通安全責任等級分級辦法修正草案

大綱

- 前言
- 政府領域聯防監控情資收容與分析
- SOC監控有效性驗證
- SOC監控有效性現況
- SOC監控防護建議
- 機關配合事項

政府領域聯防監控收容架構

政府領域聯防監控中心(G-SOC)

- 制定情資格式與收容作業規範
- 推動資通安全責任等級A/B級公務機關建立資安監控機制
- 建置情資回傳架構，收容政府機關回傳資安監控情資

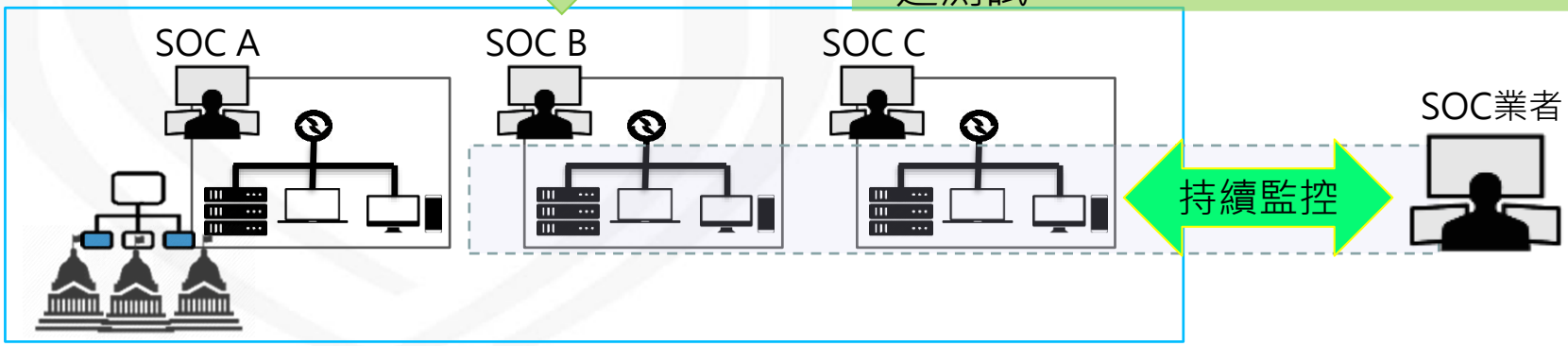
情資收容

情資回饋

情資收容

政府機關

- 機關SOC分為自建SOC與委任SOC業者
- 自建SOC機關需進行連通測試
- 委任SOC機關可由SOC業者協助進行連通測試



政府領域聯防監控情資規劃(1/3)

- 常見網路攻擊可參考駭客狙殺鍊(Cyber Kill Chain)，分為偵查、武裝、遞送、攻擊、安裝、發令與控制及採取行動等階段

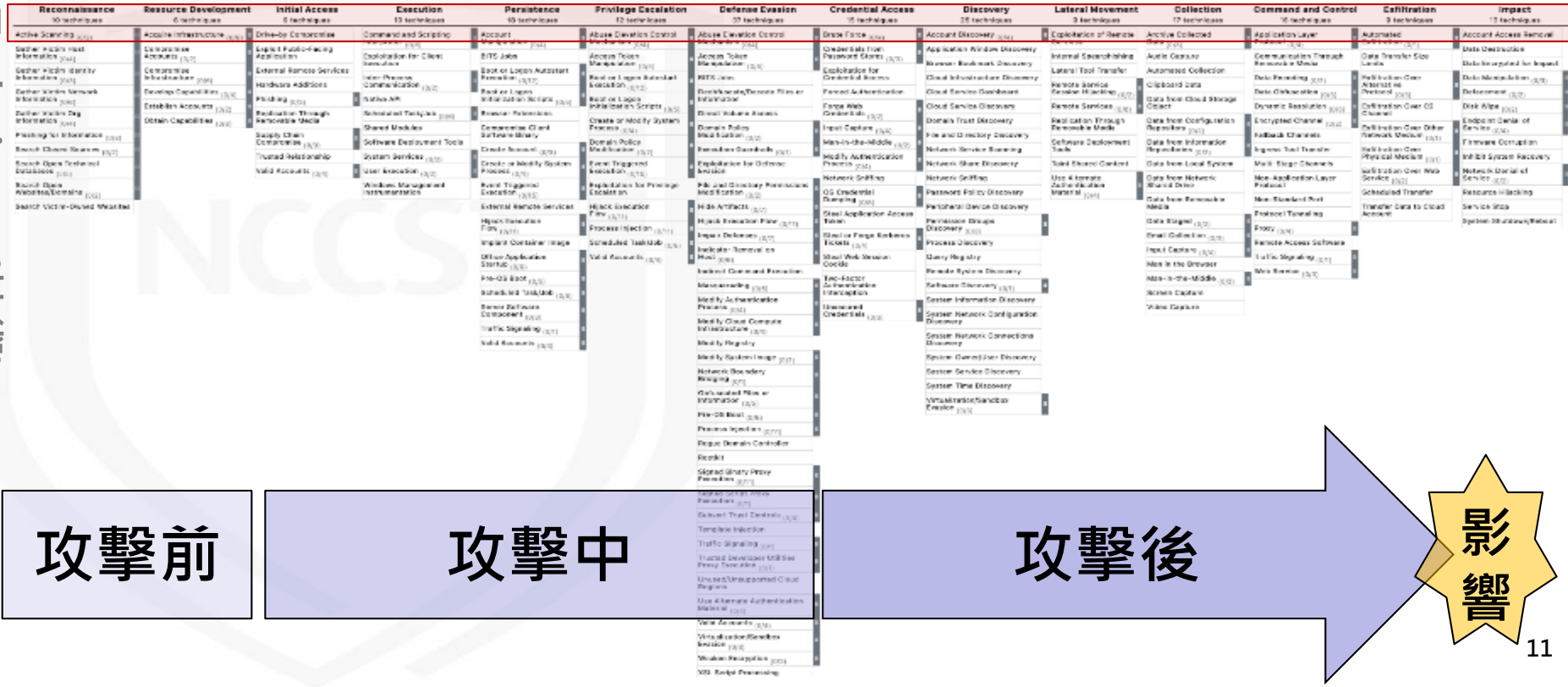
偵查 (Reconnaissance)	武裝 (Weaponization)	遞送 (Delivery)	攻擊 (Exploitation)	安裝 (Installation)	發令與控制 (Command and Control)	採取行動 (Actions on Objectives)
研究、識別及選擇目標，可以在網際網路上搜尋相關資訊，或是利用工具掃描或探測目標環境	針對特定的安全漏洞，設計遠端存取木馬程式，包裹在可遞送的資料中，多數以自動化工具產生，且利用常見資料檔案進行偽裝	設法將惡意程式傳送到目標環境，如電子郵件附件、網站及可移動的USB媒體等遞送管道	惡意程式遞送到目標主機後，將觸發內部的程式碼，以應用程式或作業系統的安全弱點為目標，開始進行攻擊	於受駭主機安裝遠端存取的木馬或後門程式，而攻擊者可繼續隱藏於受駭環境中	受駭主機須向外連結網際網路上的控制伺服器，以建立控制通道，攻擊者便可利用此通道遠端操控受駭主機	攻擊者開始採取行動，如竊取資料、破壞資料的完整性與可用性、或是做為入侵其他系統的跳板

政府領域聯防監控情資規劃(2/3)

- 政府領域資安聯防監控，針對駭客狙殺鍊攻擊前、中、後等階段進行防護策略部署，並透過資安監控機制偵測相關威脅行為

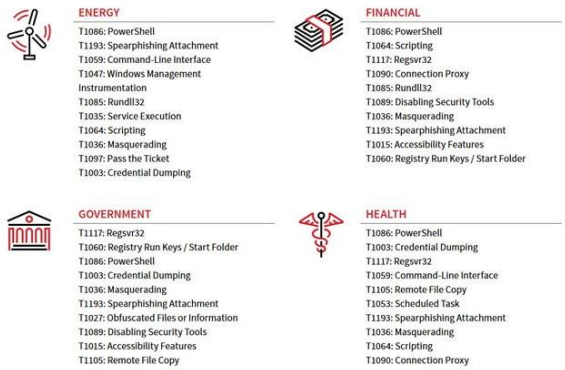
Tactics(戰略) →

Techniques(技術) ↓



政府領域聯防監控情資規劃(3/3)

- 針對駭客狙殺鍊眾多資安威脅，使用統一知識庫作為參考
  - 國外網路安全公司Red Canary分析相關產業遭受到攻擊，其中政府領域常見威脅如下
    - 利用魚叉式網路釣魚作為攻擊進入點
    - 利用PowerShell指令操控電腦
    - 利用工具竊取受駭主機認證資訊
    - 利用Pass the Ticket手法進行橫向擴散



- 面對資安相關威脅，機關可參考MITRE ATT&CK框架，評估現行資安防護項目與資安服務監控是否足夠

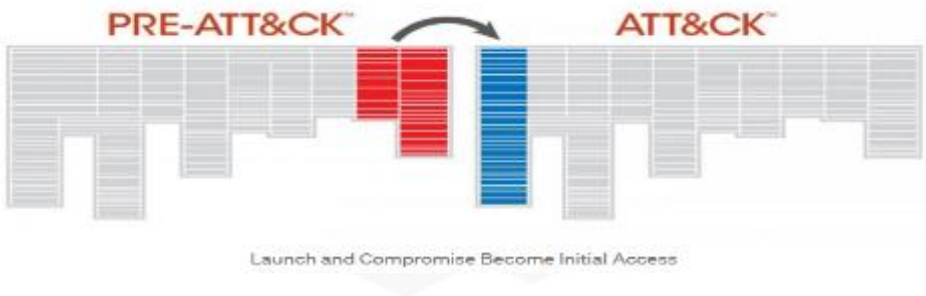
MITRE ATT&CK(1/4)

- MITRE於105年提出ATT&CK，描述攻擊者行為之知識庫框架
  - 該框架彙整眾多駭侵組織攻擊行為，並建立共通描述語言，涵蓋攻擊前、中、後之入侵戰略、技術及流程(TTP: Tactics, Techniques, and Procedures)，並對應至駭客狙殺鍊(Cyber Kill Chain)，可作為機關強化資安防護之參考
  - 可協助機關掌握近期資安風險分類與對應，評估相關防護措施是否均已涵蓋，若有缺漏與不足之處需編列資源，強化防護能量

ATT&CK：Adversarial Tactics, Techniques and Common Knowledge

MITRE ATT&CK(2/4)

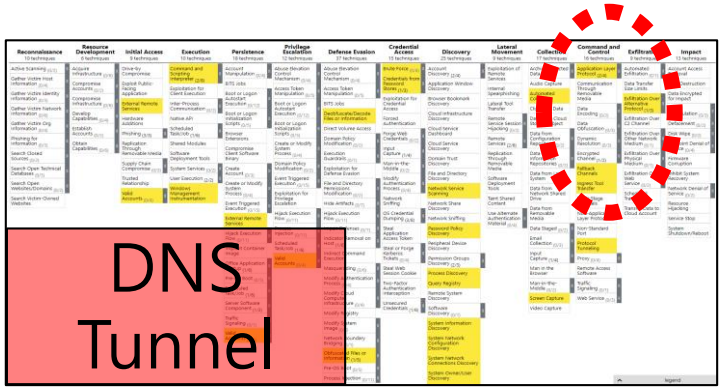
- 110年4月發布Version 9最新版
  - 共計185項(新增7項威脅手法)
  - 為完整呈現Cyber Kill Chain，整合原先PRE-ATT&CK，增加偵查(資訊蒐集)與資源開發(工具開發)，並汰除不夠精確與重複之技術項目
  - 技術(Technique)下擴充子技術(Sub-technique)項目，更細緻化描述各式攻擊技術之實行方式，並提供防護建議
  - 公布適用於工控系統之攻擊者行為知識庫(ICS-ATT&CK)



原有 ATT&CKMatrix	現有 ATT&CKMatrix
Enterprise-ATT&CK	Enterprise-ATT&CK
PRE-ATT&CK	ICS-ATT&CK
Mobile-ATT&CK	Mobile-ATT&CK

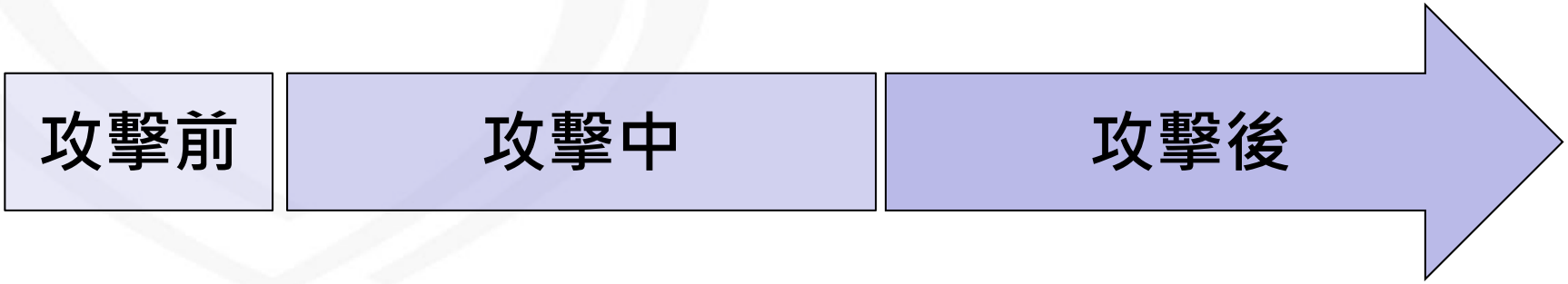
MITRE ATT&CK(3/4)

- 機關可使用ATT&CK知識庫框架之應用建議
  - 109年5月經檢視聯防監控情資，觀測到跨機關新興威脅手法，經濟能源體系遭使用相同之Cobalt Strike與DNS Tunnel手法，進行相關駭客工具下載、入侵及控制樣態
  - 機關可使用ATT&CK，評估現行資安監控與防護涵蓋度
    - 是否針對DNS Tunnel行為或內網擴散進行偵測與防護



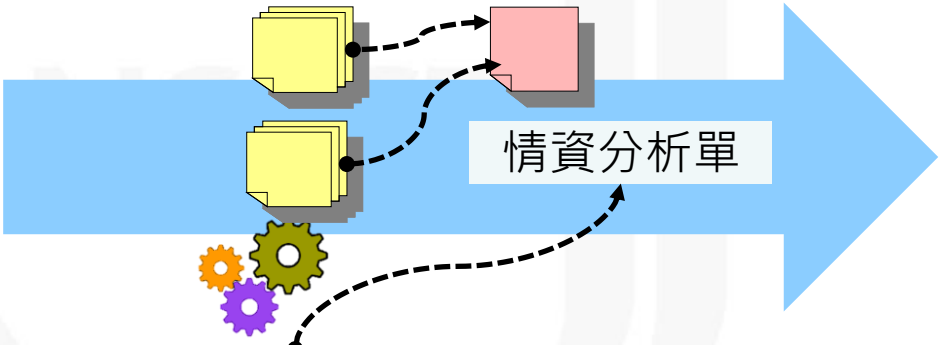
MITRE ATT&CK(4/4)

- 評估威脅嚴重程度與部署相關防護建議
  - 若機關發生之事件分類為”攻擊前”階段手法
    - 可掌握機關常遭受攻擊之進入點，並檢視相關防護機制是否運作正常
  - 若機關發生之事件分類為”攻擊中”階段手法
    - 應分析與確認相關遭攻擊之主機系統是否遭攻擊成功並造成影響
  - 若機關發生之事件分類為”攻擊後”階段之手法，代表機關可能需進行整體內部網段調查
    - 可使用攻擊手法對應之防護建議，進行偵測



政府領域聯防監控情資格式(1/2)

- 政府領域聯防監控(G-SOC)情資格式納入駭客狙殺鍊(Cyber kill Chain)與MITRE ATT&CK知識庫，強化威脅偵測與情資萃取能量
- 作業規範與格式已於109年7月公布於技服中心官網之聯防監控專區



- 具備受駭偵測指標(IOC)與威脅攻擊指標(IOA)
- 威脅手法分析情資
- 跨機關關聯性事件情資
- 重大資安弱點資訊

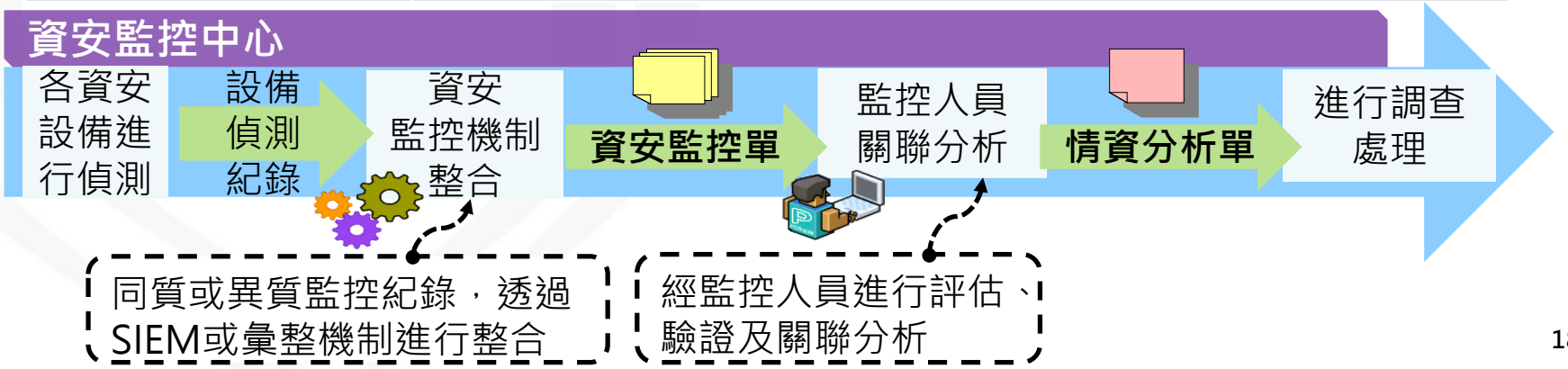
Attacker behaviours

ATT&CK Sightings

政府領域聯防監控情資格式(2/2)

- G-SOC收容情資涵蓋以下三項類型

情資內容	情資說明
資安監控單	SOC機制整合產製之資安監控單(如incident等) • 12項必填、8項選填
情資分析單	SOC分析人員對「資安監控單」進行影響性評估，提供給客戶進行分析之情資(如ticket等) • 14項必填、27項選填
監控設備狀況單	所有監控設備之監控狀況資訊 • 7項必填、1項選填 • 每月統計監控設備之監控狀況資訊



資安聯防監控情資產製應用(1/6)

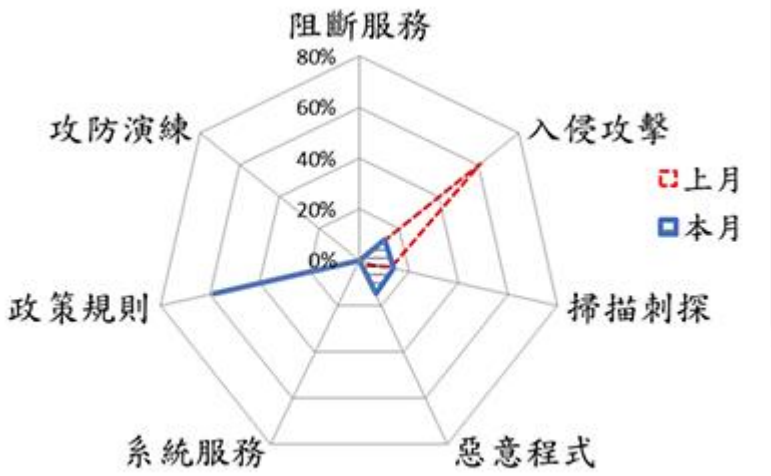
- 政府領域彙整跨機關情資與自建威脅情蒐機制，產製資安聯防監控月報
  - 提供政府機關整體事件綜覽與防護建議
  - 近期威脅事件/防護策略：提供防護/應變策略規劃參考
  - 政府威脅趨勢、專題式威脅手法分析
  - 入侵偵測與威脅防護指標

情資內容	情資說明
資安聯防監控月報	彙整樣態分析、機關威脅評估 • 跨機關監控綜覽 • 跨機關威脅種類分析 • 聯防監控回饋建議

資安聯防監控情資產製應用(2/6)

- 威脅種類分析
  - 威脅種類：統計各業務類別機關整體威脅類型趨勢變化
  - 交叉分析：依機關類型與事件類別進行交叉分析，評估各類型機關資安威脅狀況

威脅趨勢變化



跨資安責任等級交叉分析

類別 / 業務	入侵攻擊類	惡意程式類	阻斷服務類	掃描刺探類	政策規則類	系統服務類	尚需調查類	攻防演練類	合計
A級機關	30.0	32.8	7.1	202.7	564.2	20.7	51.8	0.9	909.3
	31.3	37.9	17.0	271.2	135.7	36.1	47.6	1.4	576.8
B級機關	45.7	10.9	0.7	39.6	15.9	3.8	98.0	0.2	214.7
	46.5	12.5	0.6	39.5	13.6	3.8	12.1	0.6	128.6
C級機關	0.0	0.8	0.0	1.5	0.3	0.2	0.4	0.0	3.3
	0.0	0.6	0.0	1.5	0.4	0.1	0.5	0.0	3.3
D級機關[8]	0.0	0.0	0.0	0.1	0.1	0.0	0.0	0.0	0.2
	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1
E級機關	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
合計	75.7	44.5	7.8	243.9	580.5	24.8	150.3	1.0	1127.5
	77.9	51.1	17.6	312.2	149.7	40.1	60.2	2.0	708.8

資安聯防監控情資產製應用(3/6)

重點關注威脅類型分析

編號	資安威脅類別	主要機關業務類別	主要觸發資訊
1	系統服務類	內政衛福勞動	• 網頁連線異常
2	入侵攻擊類	外交國防法務 綜合行政	• 非本國 IP 攻擊行為 • 已知中繼站網域連線
3	阻斷服務類	財政主計金融 內政衛福勞動	• 防火牆服務阻斷攻擊 • 單一來源對目標主機進行通訊埠掃描行為 • 發現阻斷服務攻擊事件
4	惡意程式類	綜合行政	• 內部主機單次連線至惡意 IP • 後門/間諜程式連線行為
5	政策規則類	外交國防法務	• 單一IP 4 小時內嘗試使用 2 個以上帳號進行登入
6	掃描刺探類	綜合行政 內政衛福勞動	• 外部主機執行掃描探測攻擊 • 高風險事件偵測
7	尚需調查類	綜合行政	• 防火牆威脅事件
8	經同意之攻防演練類	綜合行政 教育科學文化	• 疑似技服滲透測試事件

跨機關威脅種類趨勢變化

表13 各業務類別與威脅種類交叉分析

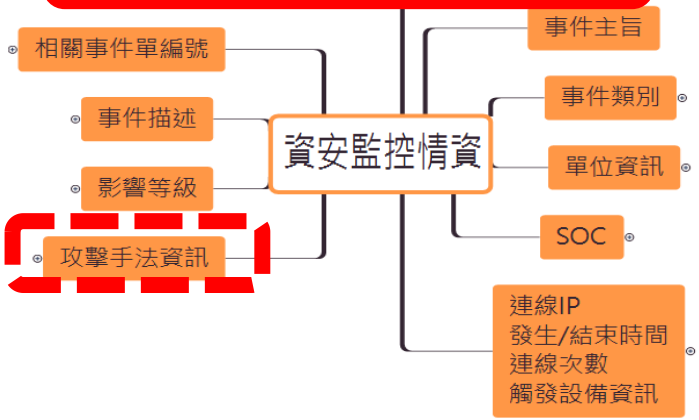
類別 / 業務	入侵攻擊類	惡意程式類	阻斷服務類	掃描刺探類	政策規則類	系統服務類	尚需調查類	攻防演練類	合計
綜合行政	3.7	0.6	0.0	3.0	0.3	0.1	17.8	0.0	25.6
	2.6	0.6	0.0	2.7	0.4	0.6	12.0	0.0	18.9
內政衛福勞動	11.0	2.1	0.1	27.6	4.4	1.1	4.9	0.0	51.2
	1.1	5.0	0.3	36.1	18.7	2.7	15.9	0.0	79.9
外交國防法務	38.0	1.1	0.0	6.2	14.8	0.1	3.4	0.0	63.6
	72.7	1.5	0.0	7.0	14.8	0.0	3.4	0.0	99.5
交通環境資源	0.0	4.4	0.2	6.1	4.4	0.0	2.0	0.0	17.0
	0.1	5.1	0.0	6.0	5.8	0.0	2.3	0.0	19.3
財政主計金融	4.1	0.5	0.4	18.0	1.0	0.3	1.3	0.0	25.6
	4.0	0.7	0.9	21.4	1.7	1.7	2.4	0.0	32.9
經濟能源農業	0.2	3.7	0.1	5.9	25.7	0.4	25.4	0.0	61.4
	0.6	19.2	0.2	7.2	16.4	0.6	13.9	0.0	58.0
教育科學文化	0.7	1.6	0.9	15.3	21.7	1.5	13.4	0.0	55.1
	0.9	1.3	0.8	15.1	18.1	1.3	21.3	0.0	58.9
非行政院所屬	7.0	7.9	0.0	3.3	11.6	0.1	0.5	0.0	30.6
	3.1	4.3	0.1	3.4	7.6	0.1	0.5	0.0	19.1

資安聯防監控情資產製應用(4/6)

- 萃取並回饋入侵偵測與威脅防護指標，提供跨機關偵測、分析及聯防使用

情資內容	情資說明
威脅清單(聯防監控指標)	• 受駭偵測指標(IOC) • 威脅攻擊指標(IOA) • IP/DN/URL Watchlist

威脅與攻擊手法由相關資訊欄位進行萃取



威脅樣態
Struts2網頁框架漏洞利用手法受駭偵測指標
社交工程郵件手法CVE-2017-11882受駭偵測指標
Powershell之無檔案類威脅受駭偵測指標
中國菜刀網頁型後門攻擊指標
DNS Tunneling攻擊手法與指標

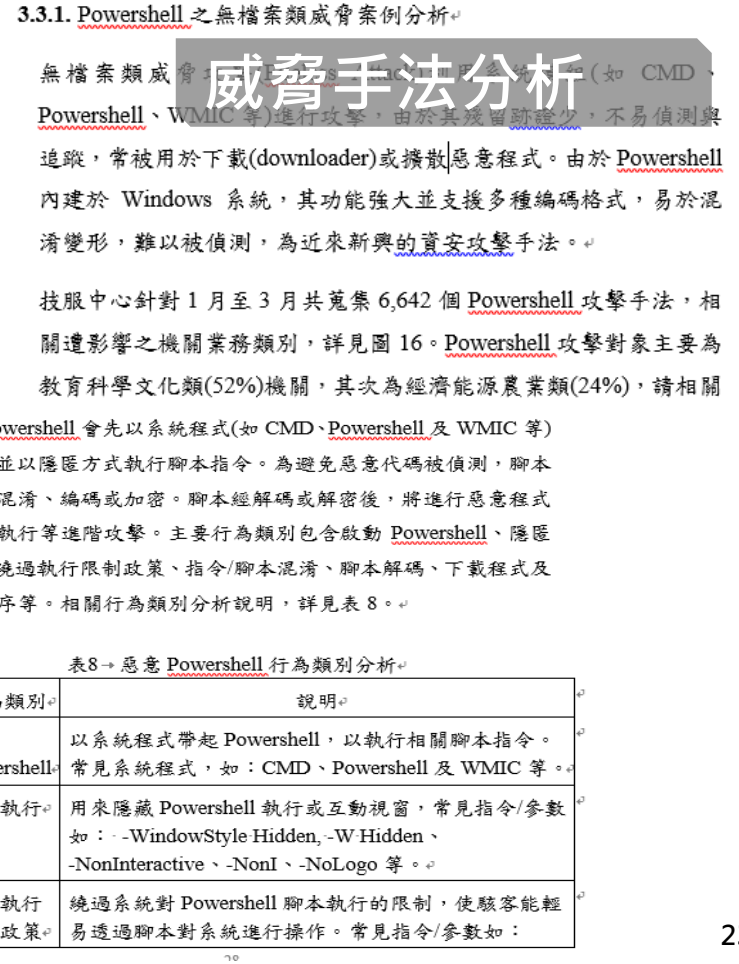
編號	IP	國別	附註/掃描 IP 數量
1	[redacted]	TW	實際入侵並影響機關
2	[redacted]	HK	實際入侵並影響機關
3	[redacted]	CN	36

```
<stix:Indicators>
    <stix:Indicator id="example:indicator-91d64e67-4e19-4e68-90cf-3e1c5ac637f1" times
        <indicator:Title>Malicious IP Indicator</indicator:Title>
        <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">IP Watchlist</ir
        <indicator:Description>This indicator is extracted from a powershell command.
        <indicator:Observable id="example:Observable-3df06013-d59e-4fc7-a1a4-0fe1db43
            <cybox:Object id="example:Address-1fb49c86-6ea7-49e9-b29f-a2d3610faeba">
                <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="i
                    <AddressObj:Address_Value condition="Equals">[redacted]</Address
                </cybox:Properties>
```

資安聯防監控情資產製應用(5/6)

- 聯防監控回饋建議
  - –針對近期整體跨領域/機關觀測到網路威脅與攻擊手法，進行手法分享與提供防護策略

威脅事件手法分享/防護策略
Apache Struts2漏洞(CVE-2017-5638)遭利用植入挖礦程式
D-Link特定無線路由器存在資訊洩漏疑慮
Smominru殭屍網路程式進行虛擬貨幣挖礦行為
Memcached分散式快取系統遭利用作為DDoS放大攻擊
惡意電子郵件手法分析 -CVE-2017-11882 -CVE-2017-0199 -LokiBot
Powershell之無檔案類威脅案例分析



威脅手法分析

3.3.1. Powershell 之無檔案類威脅案例分析

無檔案類威脅[illegible]（如 CMD、Powershell、WMIC 等）進行攻擊，由於其殘留跡證少，不易偵測與追蹤，常被用於下載(downloader)或擴散惡意程式。由於 Powershell 內建於 Windows 系統，其功能強大並支援多種編碼格式，易於混淆變形，難以被偵測，為近來新興的資安攻擊手法。

技服中心針對 1 月至 3 月共蒐集 6,642 個 Powershell 攻擊手法，相關遭影響之機關業務類別，詳見圖 16。Powershell 攻擊對象主要為教育科學文化類(52%)機關，其次為經濟能源農業類(24%)，請相關

惡意 Powershell 會先以系統程式(如 CMD、Powershell 及 WMIC 等)啟動，並以隱匿方式執行腳本指令。為避免惡意代碼被偵測，腳本會進行混淆、編碼或加密。腳本經解碼或解密後，將進行惡意程式下載與執行等進階攻擊。主要行為類別包含啟動 Powershell、隱匿執行、繞過執行限制政策、指令/腳本混淆、腳本解碼、下載程式及執行程序等。相關行為類別分析說明，詳見表 8。

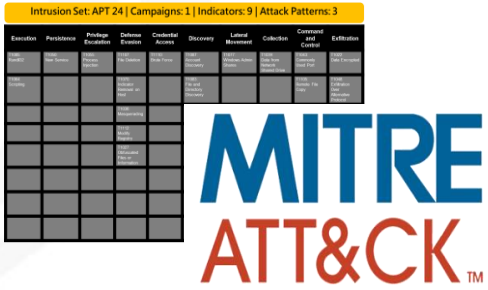
表8 惡意 Powershell 行為類別分析

編號	行為類別	說明
1	啟動 Powershell	以系統程式帶起 Powershell，以執行相關腳本指令。常見系統程式，如：CMD、Powershell 及 WMIC 等。
2	隱匿執行	用來隱藏 Powershell 執行或互動視窗，常見指令/參數如：-WindowStyle Hidden, -W Hidden、-NonInteractive、-NonI、-NoLogo 等。
3	繞過執行限制政策	繞過系統對 Powershell 腳本執行的限制，使駭客能輕易透過腳本對系統進行操作。常見指令/參數如：

資安聯防監控情資產製應用(6/6)

- 108年6月起，政府領域資安聯防監控月報參考MITRE ATT&CK框架，提供資安威脅偵測與防護建議，涵蓋新興威脅、後門連線及命令控制等手法
  - –11項ATT&CK攻擊階段(Tactic)
  - –33項ATT&CK攻擊手法(Technique)

研究案例套用
MITRE ATT&CK資安框架
並回饋予資安聯防監控月報



資安聯防監控月報應用建議

- 月報案例應用
  - 了解新興資安威脅，檢視機關資安防護機制是否有效監控並阻擋相關威脅，並參考技服中心防護建議，調整機關內部環境

- 威脅指標部署
  - 涵蓋政府領域高風險威脅、社交工程郵件、殭屍網路威脅及新興資安威脅等，建議機關評估相關威脅，並部署於資安防護機制

- 資安意識提升
  - 提供月報予機關內部同仁，提升資安意識，強化機關資安防護

小結

- 機關應依資通安全管理法規定建置資安防護機制，並依所面臨威脅情況建置資安偵蒐機制，並納入監控範圍
- 針對資安聯防監控月報相關情資，建議可進行下列應用
  - 部署威脅指標至相關防護機制，掌握機關資安風險
  - 了解目前監控防護機制針對威脅之涵蓋度，責成SOC業者部署相關偵測與分析規則
  - 針對月報新興威脅手法進行了解，提升資安防護意識

大綱

- 前言
- 政府領域聯防監控情資收容與分析
- SOC監控有效性驗證
- SOC監控有效性現況
- SOC監控防護建議
- 機關配合事項

SOC監控有效性發展歷程

- 109年起開始推動政府領域SOC監控有效性驗證，提升SOC業者執行資安監控能量與品質
  - 109年10月起試行，每月提供驗證結果予SOC業者進行改善
  - 試行結果提供資安服務廠商評鑑參考，協助業者進行改善
- 依據第六期國家資通安全發展方案，持續推動政府領域聯防監控有效性驗證
  - 110年正式列為資安服務廠商評鑑評分項目
  - 驗證結果每季公布於聯防監控月報供政府機關參考

SOC監控有效性驗證

- 針對SOC監控有效性進行驗證
  - 政府機關：推動完善監控範圍
    - 定期檢視機關填報與回傳之資安防護項目資訊，掌握防護涵蓋度
    - 若監控範圍有異動，應於管考系統即時更新
  - SOC業者：依回傳能力、偵測能力及情資品質，驗證監控成效

對象	推動項目
政府機關	完善監控範圍 • 要求機關將規定之資通安全防護項目與核心資通系統(含AD)納入監控範圍 • 檢視監控範圍涵蓋程度 • 透過SOC業者每月回傳之監控設備狀況單，掌握監控範圍運作概況
SOC業者	追蹤SOC監控成效，納入資安服務廠商評鑑之評分項目 • 回傳能力 • 偵測能力 • 情資品質

SOC監控有效性評估指標

- 政府領域SOC監控有效性評估指標分為3大類，包含回傳能力、偵測能力及情資品質

項目	評估指標
1.回傳能力	1.1資安監控情資格式與回傳率
	1.2資安防護項目回傳率
2.偵測能力	2.1網路攻防演練驗證
	2.2技服中心資安警訊驗證
	2.3機關通報資安事件驗證
3.情資品質	3.1資安監控情資品質分析
	3.2資安監控情資回饋能量

回傳能力

- 資安監控情資格式與回傳率
  - 依據SOC業者回傳之聯防監控情資內容，是否合乎格式規範並即時回傳
  - 驗證方式
    - 依據制定之規範，驗證欄位與格式是否符合
- 資安防護項目回傳率
  - 依據SOC業者回傳監控設備狀況單之資安防護項目資訊，評估其監控偵測之回傳情形
  - 驗證方式
    - 使用監控設備狀況單之資安防護項目資訊，比對SOC業者回傳之情資，是否涵蓋相關資安防護項目

偵測能力(1/2)

- 網路攻防演練驗證
  - 了解SOC業者回傳之情資，是否偵測到網路攻防演練活動，並告知機關進行通報
  - 驗證範圍
    - 蒐集網路攻防演練共65個演練機關，包含中央部會、地方政府及一級機關
  - 驗證方式
    - 使用網路攻防演練對外網段IP資訊，與SOC業者回傳之SOC情資分析單進行關聯

偵測能力(2/2)

- 技服中心資安警訊驗證
  - 以資安警訊評估SOC業者對已知資安事件之監控成效
  - 驗證方式
    - 使用技服中心之入侵攻擊情報(INT)資安警訊資訊(不含網路攻防演練)，比對SOC業者回傳之情資分析單，分析是否有效偵測相關事件
- 機關資安事件通報驗證
  - 以機關資安事件通報資訊，了解SOC業者開單之落實性
  - 驗證方式
    - 依據機關資安事件通報資訊，比對SOC業者之情資分析單，分析是否回傳相關監控情資

情資品質

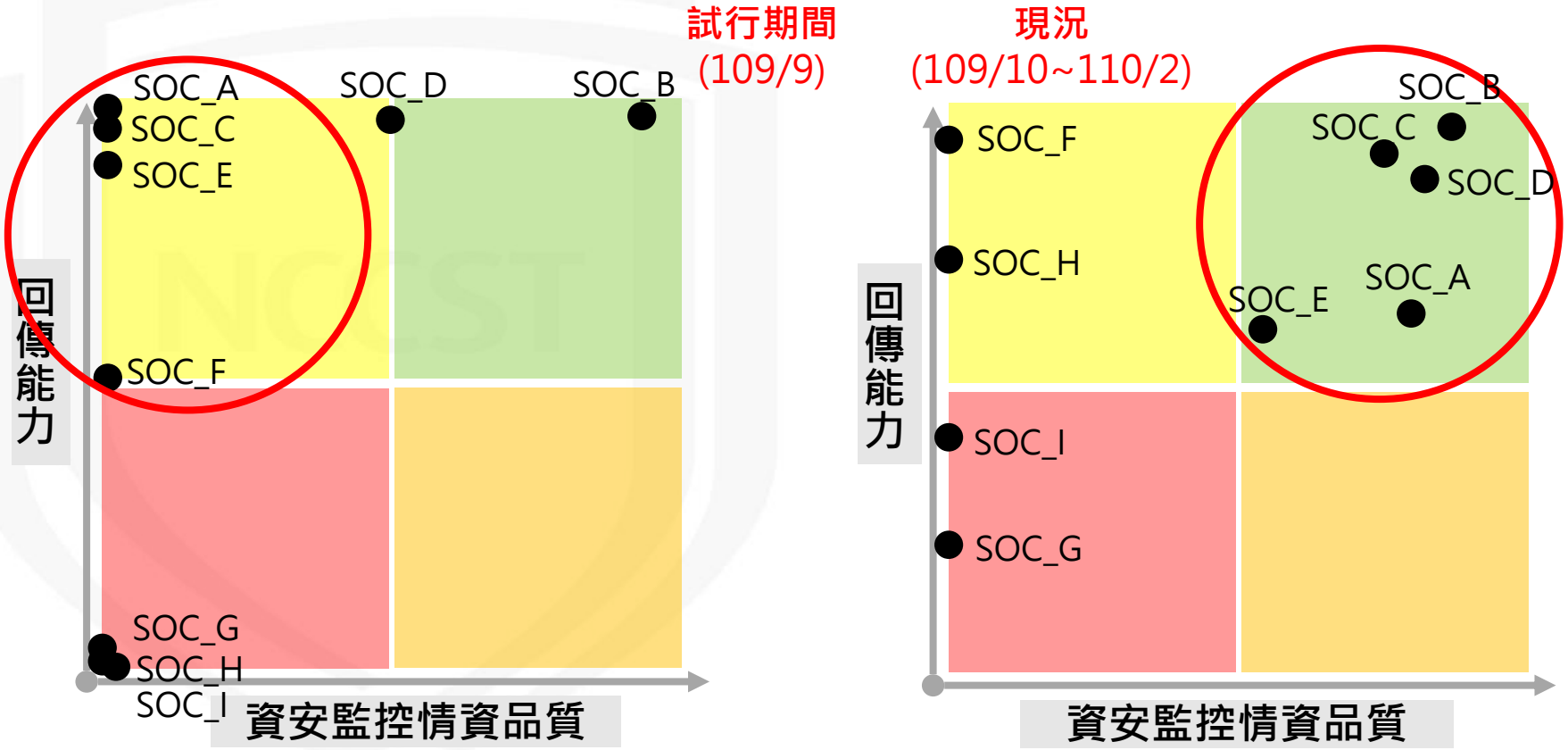
- 資安監控情資品質分析
  - 依據SOC業者回傳之聯防監控情資內容，進行品質分析
  - 驗證方式
    - 驗證內容正確性、有效情資回傳率，並評估是否有萃取分析之指標情資，包含受駭偵測指標(IOC)、威脅攻擊指標(IOA)等
- 資安監控情資回饋能量
  - 依據SOC業者回傳之聯防監控情資內容，分析是否回饋額外情資
  - 驗證方式
    - 評估有無額外回饋資訊，包含駭客狙殺鍊分類資訊(Cyber Kill Chain, CKC)、MITRE ATT&CK、駭客工具、威脅手法分析情資、跨機關關聯性事件情資或重大資安弱點資訊等，據此分析其涵蓋率

大綱

- 前言
- 政府領域聯防監控情資收容與分析
- SOC監控有效性驗證
- SOC監控有效性現況
- SOC監控防護建議
- 機關配合事項

SOC監控有效性現況(1/3)

- 回傳能力指標現況(109/10~110/2)
  - –SOC業者之資安監控情資回傳能力與品質逐步提升，已有5家SOC業者穩定回傳，具備初步萃取指標情資能力



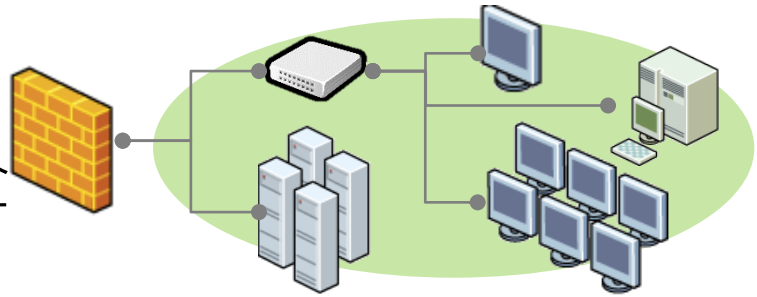
SOC監控有效性現況(2/3)

- 偵測能力指標現況：機關回報未納入監控範圍比例如下，顯見監控範圍急需檢視改善
  - 網路攻防演練48.1%
  - 技服中心資安警訊58%
  - 機關通報資安事件45%

偵測能力項目	未納入監控範圍比例
網路攻防演練	48.1%(共27則)
技服中心資安警訊	58%(共112則)
機關通報資安事件	45%(共91則)

統計區間：109/10~110/2

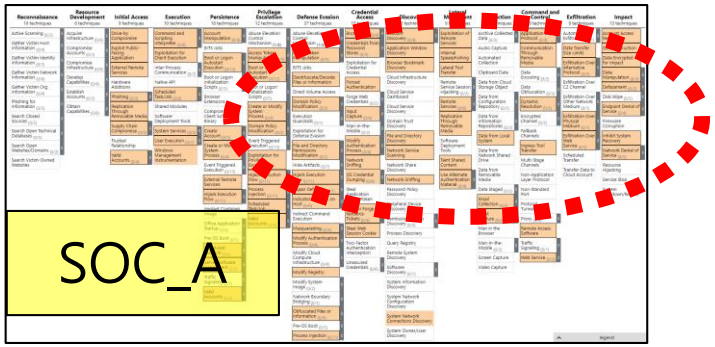
- 監控範圍認定
  - 資訊資產是否在資通安全防護項目監控範圍內
  - 機關應於資安事件結報流程，填寫受駭主機是否納入監控範圍

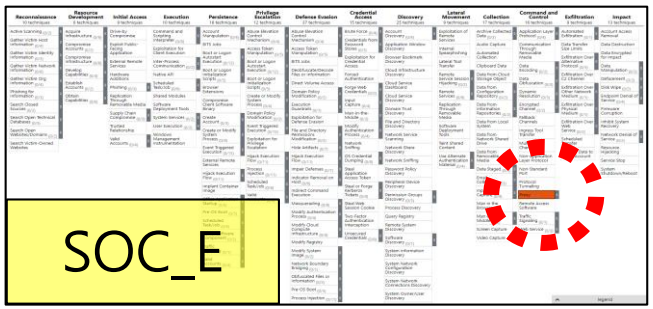


SOC監控有效性現況(3/3)

- ATT&CK威脅手法涵蓋率統計(109/10~110/2)
  - 已有2家SOC業者回饋之ATT&CK情資相對成熟
    - 部分SOC業者涵蓋率低(0.5%)，無法突顯偵測能力
  - 仍有4家SOC業者尚未回饋ATT&CK情資
  - 可透過涵蓋率了解機關現行資安防護涵蓋範圍，依重要性補足缺漏之處

SOC業者	ATT&CK 威脅手法項目涵蓋率	情資分析單數量
SOC_A	39%(70/178)	162,881
SOC_B	21%(37/178)	15,751
SOC_C	1%(2/178)	12
SOC_D	1%(2/178)	1
SOC_E	0.5%(1/178)	2,239





SOC監控有效性驗證結果

- SOC監控有效性於110年正式列為資安服務廠商評鑑評分項目
  - 相關指標驗證結果每季亦同步公布於資安聯防監控月報
    - 1、4、7、10月公布

編號	資安監控服務廠商	回傳能力			監控偵測能力			資安監控情資品質		
		資安監控單正確率	情資分析單正確率	資安防護項目回傳率	網路攻防演練驗證開單率	技服中心資安警訊驗證開單率	機關資安事件通報驗證開單率	資安監控情資欄位有誤數量	萃取分析之重要情資	額外回饋情資
1	SOC A	大部分正確 (98%)	完全正確 (100%)	少部分符合 (272%)	無結報資訊	無結報資訊	0%	1 個欄位錯誤	☐	☐
		大部分正確 (97%)	大部分正確 (97%)	未符合(0%)	無結報資訊	無結報資訊	無結報資訊	未回傳	☐	☐
2	SOC B	完全正確 (100%	少部分正確	少部分符合	無結報資訊	無結報資訊	0%	完全正確	☐	☐
		過半正 (70%								
3	SOC C	大部分 (99%								
		大部分 (99%								
4	SOC D	100.00								
		大部分 (98%								
5	SOC E	大部分正確 (98%)	過半正確 (66%)	完全符合 (100%)	0%	無結報資訊	無結報資訊	1 個欄位錯誤	■	■
		大部分正確 (97%)	大部分正確 (99%)	未符合(0%)	無結報資訊	無結報資訊	無結報資訊	未回傳	☐	☐
6	SOC F	無正確(0%)	未回傳	未符合(0%)	無結報資訊	無結報資訊	無結報資訊	未回傳	☐	☐
		少部分正確 (4%)	少部分正確 (4%)	未符合(0%)	無結報資訊	無結報資訊	無結報資訊	未回傳	☐	☐
7	SOC G	大部分正確 (99%)	少部分正確 (56%)	少部分符合 (28%)	0%	無結報資訊	無結報資訊	完全正確	☐	☐
		過半正確 (83%)	大部分正確 (92%)	未符合(0%)	無結報資訊	無結報資訊	無結報資訊	未回傳	☐	☐
8	SOC H	無正確(0%)	未回傳	未符合(0%)	無結報資訊	無結報資訊	無結報資訊	未回傳	☐	☐
		無正確(0%)	無正確(0%)	未符合(0%)	無結報資訊	無結報資訊	無結報資訊	未回傳	☐	☐

大綱

- 前言
- 政府領域聯防監控情資收容與分析
- SOC監控有效性驗證
- SOC監控有效性現況
- SOC監控防護建議
- 機關配合事項

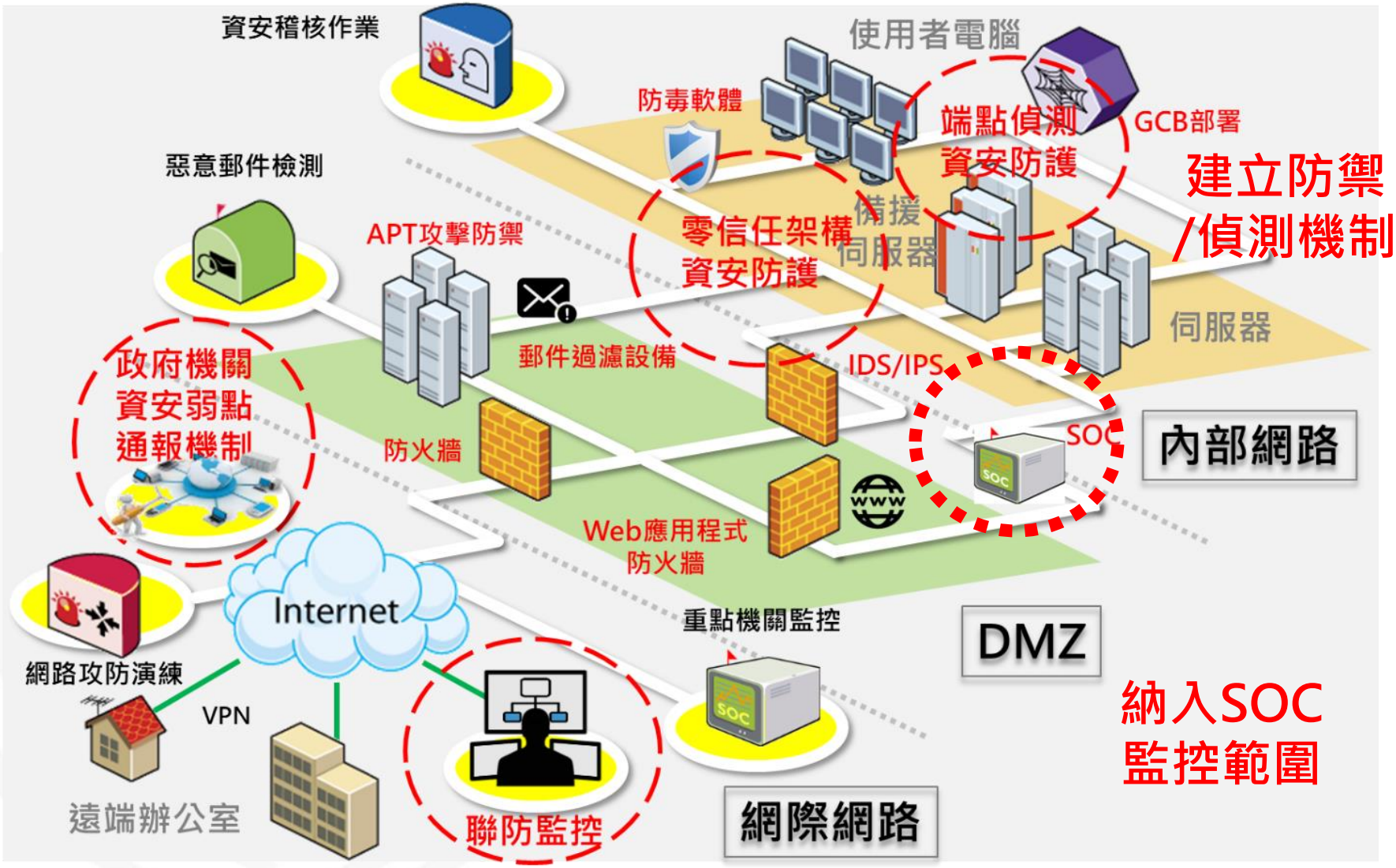
強化資安防護能量

- 目前A、B級機關大多已建置SOC監控機制，惟仍常發生資安事件
- 相關防護建議
  - 強化縱深防禦能量
  - 妥善處理監控告警 / 資安警訊事件

加強縱深防禦機制

- 完善機關資產管理與組態設定管理
  - 落實資產盤點(如VANS機制等)
  - 組態設定管理(GCB)與更新
- 部署機關內部網路端點偵測機制
  - 安裝防毒軟體 / 端點防護機制
  - 收容主機事件日誌 / 網頁日誌 / DNS日誌
- 強化機關邊境防護 / 管制
  - 適當部署資安防護項目，如WAF與IDS/IPS等
  - 將資安防護項目納入SOC監控範圍

政府機關縱深防禦示意圖



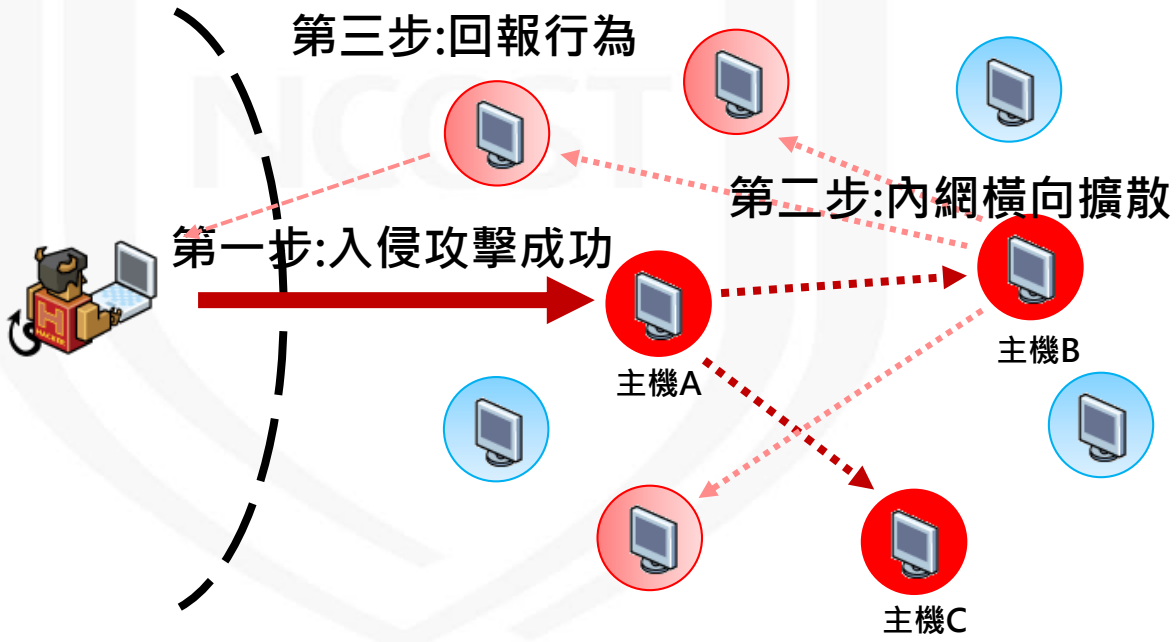
強化資安聯防體系

監控告警 / 資安警訊事件處理

- 由於駭客會透過受駭主機進行內網橫向擴散，機關常僅調查與處置告警之主機，導致威脅擴散
  - 需進行受駭影響層面評估
    - 收到SOC業者監控告警，需與SOC業者確認可能受駭標的與範圍，進行影響性評估
  - 需注意內網橫向擴散情形
    - 搭配資訊資產與端點偵測進行關聯分析，注意是否有內網橫向擴散情形，並針對所有受駭標的進行處置，避免造成更嚴重的資安事件發生

資安事件案例分享

- 駭客從外網成功入侵並使用regeorg後門進行橫向擴散，SOC業者於防火牆偵測主機A觸發大量內部異常連線行為，並告警機關
  - 機關第一時間僅處理主機A，忽略橫向擴散，導致後續受駭範圍擴大



- 針對**橫向擴散徵兆**，強化資安防護策略
- **使用regeorg proxy工具**
- **AD出現主機登入大量內網主機事件**
- **端點偵測到下載密碼竊取工具(mimikatz)或提權工具(juicyPotato)**
- **相關工具與手法，極有可能為橫向擴散徵兆**

資安監控防護建議

- 依據駭客狙殺鍊，針對不同攻擊階段可參考以下防護建議

縱深防禦

- 建立資產管理/弱點管理機制(VANS)
- **部署對應的資安防護項目(Protect)**
- 落實安全性更新與組態設定(GCB)

偵測與應變

- **確保資安防護項目與重要資產納入監控範圍**
- 強化事件處理與協防成效，以**即時阻斷**攻擊
- **針對SOC業者告警進行應變處理**
- **防堵橫向擴散跡象**

持續改善

- 針對資安事件進行**根因分析**，強化資安防護策略
- **參考聯防監控月報，強化新興攻擊防禦涵蓋度**

大綱

- 前言
- 政府領域聯防監控情資收容與分析
- SOC監控有效性驗證
- SOC監控有效性現況
- SOC監控防護建議
- 機關配合事項

機關配合事項

- 建置資安防護項目並回傳監控情資
  - –即時更新管考系統之監控範圍異動資訊
  - –責成SOC業者落實情資回傳作業與情資品質

- 參考聯防監控情資加強資安防護
  - –參考聯防監控月報，針對新興威脅強化防護策略
  - –針對SOC業者告警進行應變處理，阻斷駭客狙殺鍊
  - –針對資安事件，強化內部橫向擴散之防護機制

- 應用ATT&CK知識庫強化防護能量
  - –評估威脅嚴重程度與部署相關防護建議
  - –將情資對應ATT&CK，強化聯防監控能量

報告完畢
敬請指教